

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakaatuh

Alhamdulillah Rabbil 'alamiin segala puji dan syukur atas kehadiran Allah SWT, yang telah memberi rahmat, tuntunan dan kemurahan-Nya hikmat dalam pengerjaan Proyek Akhir ini. Proyek Akhir yang berjudul “Perancangan Dan Implementasi IPS(*Intrusion Prevention System*) Berbasis Web Menggunakan Snort Dan Iptables” dengan segala kekurangan dan kelebihanannya dan merupakan salah satu syarat untuk memperoleh gelar Diploma Teknik Jurusan Teknik Komputer Politeknik Telkom.

Diharapkan dengan pembuatan proyek akhir ini dapat membantu dan semoga kedepannya hal ini dapat dilakukan pengembangan melalui ide-ide kreatif dari para pembaca.

Perlu disadari bahwa dalam penyusunan proyek akhir ini masih terdapat kekurangan karena berbagai keterbatasan. Untuk itu diperlukan kritik dan saran dari para pembaca yang bersifat membangun demi penyempurnaan pada penulisan berikutnya. Semoga laporan penelitian ini dapat memberikan manfaat bagi kita semua.

Wassalamu'alaikum Warahmatullahi Wabarakaatuh

DAFTAR ISI

LEMBAR PERNYATAAN.....	i
UCAPAN TERIMA KASIH.....	ii
LEMBAR PENGESAHAN	iv
ABSTRAK	v
ABSTRACT.....	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	ix
DAFTAR TABEL	x
BAB I.....	1
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah.....	2
1.3 Tujuan.....	2
1.4 Batasan Masalah.....	2
1.5 Metodologi Penyelesaian.....	3
1.6 Sistematika Penulisan	4
1.7 Jadwal Kegiatan	4
BAB II	5
LANDASAN TEORI	5
2.1 IPS(Intrusion Prevention System)[DER].....	5
2.1.1 IPS Engine[PUJ06].....	5
2.2 IDS(Intrusion Detection System)	6
2.2.1 Snort IDS[PUJ06]	6
2.3 Firewall	9
2.3.1 IPTables Firewall[PUJ06].....	10
2.4 PHP(PHP:Hypertext Preprocessor)[DOY10]	10
BAB III.....	12
PERANCANGAN SISTEM	12
3.1 Identifikasi Kebutuhan Sistem	12
3.1.1 Kebutuhan Fungsional.....	12
3.1.2 Kebutuhan Nonfungsional	13

3.2	Arsitektur Sistem.....	13
3.2.1	Arsitektur Fungsional	13
3.2.2	Arsitektur Komunikasi Perangkat Lunak	15
3.3	Skenario Pengujian Sistem	16
3.3.1	Konfigurasi Awal	16
3.3.2	Skenario Serangan.....	16
BAB IV		20
IMPLEMENTASI DAN PENGUJIAN SISTEM		20
4.1	Konfigurasi Sistem IPS.....	20
4.1.1	Instalasi Paket yang Dibutuhkan	20
4.1.2	Konfigurasi Database	20
4.1.3	Instalasi Snort.....	21
4.1.4	Konfigurasi Database	21
4.1.5	Konfigurasi Snort	21
4.1.6	Konfigurasi Base	21
4.1.7	Instalasi Blockit.....	22
4.1.8	Konfigurasi Blockit	22
4.2	Pengujian Sistem IPS.....	23
4.2.1	Uji Scanning terhadap Web Server	24
4.2.2	Uji Akses Dashboard IPS	27
4.2.3	Uji SQL Injection Terhadap Dashboard IPS	29
4.2.4	Uji Denial of Service(DoS).....	31
4.3	Pengujian Fungsionalitas	34
BAB V		36
PENUTUP.....		36
5.1	SIMPULAN	36
5.2	SARAN.....	36
DAFTAR PUSTAKA.....		37
LAMPIRAN.....		38

DAFTAR GAMBAR

Gambar 2.1 Flowchart IPS engine	6
Gambar 2.2 Bagian-Bagian IDS.....	8
Gambar 2.3 Ilustrasi <i>Firewall</i> [WIK11]	9
Gambar 3.4 Arsitektur Fungsional	14
Gambar 3.5 Arsitektur Komunikasi Perangkat Lunak	15
Gambar 3.6 Alur Pengujian Serangan	17
Gambar 4.7 Start Service	24
Gambar 4.8 Kondisi Sebelum <i>Scanning</i>	24
Gambar 4.9 Hasil <i>Scanning</i> Dengan Nmap	25
Gambar 4.10 <i>Alert Scanning</i>	25
Gambar 4.11 <i>Block Scanning</i>	26
Gambar 4.12 <i>Rule Firewall</i> Pasca <i>Scanning</i>	26
Gambar 4.13 Ping Pasca <i>Scanning</i>	26
Gambar 4.14 Kondisi Sebelum Dashboard IPS di Akses	27
Gambar 4.15 Akses Dashboard IPS oleh <i>Intruder</i>	27
Gambar 4.16 <i>Alert Web Application Attack</i>	28
Gambar 4.17 <i>Block</i> Akses Dashboard IPS.....	28
Gambar 4.18 <i>Rule Firewall</i> Pasca Akses Dashboard IPS	28
Gambar 4.19 Akses IPS Pasca Serangan	29
Gambar 4.20 Kondisi Sebelum Melakukan SQLInjection	29
Gambar 4.21 Kondisi Pasca Proses SQL Injection	30
Gambar 4.22 <i>Alert SQL Injection</i>	30
Gambar 4.23 <i>Block SQL Injection</i>	31
Gambar 4.24 <i>Rule Firewall</i> Pasca SQL Injection	31
Gambar 4.25 Ping Pasca SQL Injection	31
Gambar 4.26 Kondisi Sebelum Flooding	32
Gambar 4.27 Flooding Dengan Mega Death	32
Gambar 4.28 <i>Alert DoS</i>	33
Gambar 4.29 <i>Block Flooding</i>	33
Gambar 4.30 <i>Rule Firewall</i> Pasca Flooding	33
Gambar 4.31 Kondisi Pasca Flooding	34

DAFTAR TABEL

Tabel 1.1 Jadwal Kegiatan	4
Tabel 3.2 Kebutuhan perangkat keras	15
Tabel 4.2 Ringkasan pengujian serangan	23
Tabel 4.3 Pengujian Fungsionalitas.....	34